



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/457,732	12/10/1999	ANDREA CALIFANO	YO999-137	8003

21254 7590 03/18/2004  
MCGINN & GIBB, PLLC  
8321 OLD COURTHOUSE ROAD  
SUITE 200  
VIENNA, VA 22182-3817

EXAMINER

LAFORGIA, CHRISTIAN A

ART UNIT PAPER NUMBER

2131

DATE MAILED: 03/18/2004

7

Please find below and/or attached an Office communication concerning this application or proceeding.

## Office Action Summary

Application No.

09/457,732

Applicant(s)

CALIFANO ET AL.

Examiner

Christian La Forgia

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 02 January 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-36 is/are pending in the application.
- 4a) Of the above claim(s) 4 is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-3 and 5-36 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |   |   |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)             | 4) <input type="checkbox"/> Interview Summary (PTO-413)                     |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)    | Paper No(s)/Mail Date. _____  |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date _____   | 6) <input type="checkbox"/> Other: _____                                    |

### DETAILED ACTION

1. The amendment filed on 02 January 2004 is noted and made of record.
2. Claims 1 through 36 have been presented for examination.
3. Claim 4 has been cancelled as per Applicant's request.

#### *Response to Arguments*

4. Applicant's arguments with respect to claims 1-36 have been considered but are moot in view of the new ground(s) of rejection.
5. See further rejections that follow.

#### *Claim Rejections - 35 USC § 102*

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1-3, 9, 14-18, 20, 24-28, 30-34, and 36 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,446,210 to Borza, hereinafter Borza.
8. As per claims 1, 24, and 31, Borza teaches a method of processing semiotic data, comprising:

receiving semiotic data including a data set P (Figures 3 [block 80], 5, 7a, 7b, 10, 11, 13, 14, 15; column 2, line 52 to column 3, line 23; column 8, lines 4-28);

selecting a function h, and for at least one of each said data set P to be collected, computing h(P) (Figure 5; column 7, line 45 to column 8, line 3);

Art Unit: 2131

destroying said data set P (column 2, lines 27-29); and  
storing  $h(P)$  in a database (Figures 7a, 7b, 12; column 12, lines 39-53); and  
to determine whether P' is a predetermined subject, comparing  $h(P)$  to all available  $h(P)$ s  
to determine whether there is a match (Figure 12; column 8, lines 28-38);  
wherein said data set P cannot be extracted from  $h(P)$  (column 8, lines 28-38).

9. Regarding claims 2 and 25, Borza teaches wherein said semiotic data comprises  
biometric data (column 11, line 65 to column 12, line 18).

10. Regarding claim 3, Borza teaches wherein said function h comprises a secure hash  
function (Figure 5; column 7, line 45 to column 8, line 3).

11. As per claim 9, Borza teaches a method of processing semiotic data, comprising:  
receiving semiotic data including a data set P (Figures 3 [block 80], 5, 7a, 7b, 10, 11, 13,  
14, 15; column 2, line 52 to column 3, line 23; column 8, lines 4-28);  
selecting a function h, and for at least one of each said data set P to be collected,  
computing  $h(P)$  (Figure 5; column 7, line 45 to column 8, line 3);  
destroying said data set P (column 2, lines 27-29); and  
storing  $h(P)$  in a database (Figures 7a, 7b, 12; column 12, lines 39-53); and  
wherein said data set P cannot be extracted from  $h(P)$  (column 8, lines 28-38);  
wherein the data set P is not determined perfectly by its reading (column 11, lines 25-34),

Art Unit: 2131

wherein each reading gives a number  $P_i$ , wherein  $i$  is no less than 0, wherein  $P_0$  is for an initial reading, and a secret version of said initial reading is stored after further processing thereof (column 11, line 65 to column 12, line 34),

wherein reading  $P_0$  is different from  $P_i$  for  $i > 0$ , and the secret version of  $P_0$  is different from the secret version of  $P_i$ , such that no identification is possible by a direct comparison of the encrypted data (column 11, line 65 to column 12, line 34).

12. Regarding claims 14, 16, 18, 20, 26, 28, 30, 32, 34, and 36 Borza teaches wherein at least one of said data set  $P$  and  $P'$  comprises a personal data set (column 12, lines 25-34).

13. As per claims 15, 17, 27, and 33, Borza teaches a method of processing biometric data, comprising:

acquiring unencrypted biometric data including at least one data set  $P$  (Figure 3 [block 80]; column 8, lines 4-28);

encrypting, with one of a secure hash function and an identity function, each said at least one data set acquired (Figure 3 [block 73]; column 5, lines 42-54; column 8, lines 28-38);

destroying the unencrypted data set  $P$  (column 2, lines 27-29);

storing each of the at least one encrypted data set in a database (Figures 7a, 7b, 12; column 8, lines 28-48; column 12, lines 39-53),

wherein unencrypted biometric data is not available nor retrievable from said data stored in said database (column 8, lines 28-38),

Art Unit: 2131

to determine whether a data set P' is a predetermined subject, comparing an encrypted data set of P' to the at least one encrypted data set stored in the database to determine whether there is a match (Figure 12; column 8, lines 28-38).

***Claim Rejections - 35 USC § 103***

14. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

15. Claims 5-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Borza.

16. As per claim 5, Borza teaches a method of processing semiotic data, comprising:

receiving semiotic data including a data set P (Figures 3 [block 80], 5, 7a, 7b, 10, 11, 13, 14, 15; column 2, line 52 to column 3, line 23; column 8, lines 4-28);

selecting a function h, and for at least one of each said data set P to be collected, computing h(P) (Figure 5; column 7, line 45 to column 8, line 3);

destroying said data set P (column 2, lines 27-29); and

storing h(P) in a database (Figures 7a, 7b, 12; column 12, lines 39-53); and

wherein said data set P cannot be extracted from h(P) (column 8, lines 28-38);

the method further comprising:

selecting a private key/public key (K, k) once for all cases (column 4, lines 26-32); and

choosing said function h as the public encryption function corresponding to k (column 5, lines 28-54).

17. Borza does not teach destroying said private key K and sending said private key K to a trusted party. It would have been obvious to one having ordinary skill in the art at the time the invention was made to destroy the private key K and send it the private key K to a trusted third

Art Unit: 2131

party, since it is known in the art that the private key is needed to decrypt any message encrypted with public key  $k$ , therefore the fewer entities that have access to private key  $K$  equals the fewer number of people that can access messages encrypted with public key  $k$ .

18. Regarding claim 6, Borza teaches wherein said data set  $P$  cannot be extracted from  $h(P)$ , except by the trusted party (column 8, lines 28-38).

19. Regarding claim 7, Borza teaches further comprising:

to determine whether some  $P'$  is a predetermined subject, comparing said  $h(P)$  to all available  $h(P)$ s (column 12, lines 48-61); and

determining whether there is a match (column 12, lines 48-61).

20. Regarding claim 8, Borza does not teach wherein the trusted party comprises a panel of members, and wherein a secret is shared among the members so that only at least a predetermined number of panel members can reconstitute the secret in its entirety by putting together their share of the secret. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the trusted party to comprise of a panel of members, and share a secret is amongst the members so that only at least a predetermined number of panel members can reconstitute the secret in its entirety by putting together their share of the secret, since it has been held that mere duplication of essential elements (e.g. trusted third party) involves only routine skill in the art. *St. Regis Paper Co. v. Bemis Co.*, 193 USPQ 8. See also MPEP § 2144.04.

Art Unit: 2131

21. Claims 10-13, 19, 21-23, 29, and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Borza in view of U.S. Patent No. 6,487,662 to Kharon et al., hereinafter Kharon.

22. Regarding claim 10, Borza does not teach extracting sub-collections  $S_j$  from the collection of data in data set P; and encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability.

23. Kharon teaches further comprising:

extracting sub-collections  $S_j$  from the collection of data in data set P (Figure 6 [block 340]; column 13, lines 43-67); and

encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability (Figure 6 [block 347]; column 13, lines 43-67). It would have been obvious to one of ordinary skill in the art at the time the invention was made to sample a smaller section of the data set. One would be motivated to do because there is a better probability that a smaller area is less likely to change, therefore making it more difficult for someone to steal someone's identification.

24. With regards to claims 11 and 21, Borza does not teach comparing encrypted versions of the sub-collections  $S_j$  with those data stored in said database, wherein if one or more of the sub-collection  $S_j$  matches with said data, then verification is deemed to have occurred.

25. Kharon teaches further comprising:



Art Unit: 2131

comparing encrypted versions of the sub-collections  $S_j$  with those data stored in said database (Figure 6 [blocks 345, 347]; column 13, lines 43-67; column 14, lines 28-39; column 15, lines 42-55),

wherein if one or more of the sub-collection  $S_j$  matches with said data, then verification is deemed to have occurred (Figure 6 [blocks 345, 347]; column 13, lines 43-67; column 14, lines 28-39; column 15, lines 42-55). It would have been obvious to one of ordinary skill in the art at the time the invention was made to sample a smaller section of the data set. One would be motivated to do because there is a better probability that a smaller area is less likely to change, therefore making it more difficult for someone to steal someone's identification.

26. Concerning claims 12 and 23, Borza teaches further comprising:

each time a  $P_i$ , with  $i > 0$ , is read, computing all possible predetermined size variations of  $P_i$  which correspond to an acceptable predetermined imprecision of the reading (column 11, lines 25-34; column 12, lines 25-61); and

encrypting all such modified data, and comparing said encrypted modified data to data stored in said database (column 8, lines 28-48; column 12, lines 25-61).

27. Concerning claim 13, Borza teaches wherein for a plurality of users of the same biometric information, said biometric information is encrypted differently for each user (column 4, lines 46-58; column 5, lines 42-55).

28. As per claims 19, 29, and 35, Borza teaches a method of extracting components of biometric data which are stable under measurement errors, comprising:

Art Unit: 2131

acquiring unencrypted biometric data including at least one data set P (Figure 3 [block 80]; column 8, lines 4-28);

encrypting each said at least one data set acquired to form at least one encrypted data set (Figure 3 [block 73]; column 5, lines 42-54; column 8, lines 28-38);

destroying the unencrypted data set P (column 2, lines 27-29); and

storing each said at least one encrypted data set in a database (Figures 7a, 7b, 12; column 8, lines 28-48; column 12, lines 39-53),

wherein unencrypted biometric data is not available nor retrievable from said data stored in said database (column 8, lines 28-38).

29. Borza does not teach extracting sub-collections  $S_j$  from the collection of data in data set P; and encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability.

30. Kharon teaches further comprising:

extracting sub-collections  $S_j$  from the collection of data in data set P (Figure 6 [block 340]; column 13, lines 43-67); and

encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability (Figure 6 [block 347]; column 13, lines 43-67). It would have been obvious to one of ordinary skill in the art at the time the invention was made to sample a smaller section of the data set. One would be motivated to do because there is a better probability that a smaller area is less likely to change, therefore making it more difficult for someone to steal someone's identification.

Art Unit: 2131

31. Regarding claim 22, Borza teaches wherein the data set P is not determined perfectly by its reading, such that each reading gives a number  $P_i$ ,

wherein  $i$  is no less than 0 (column 11, line 65 to column 12, line 34),

wherein  $P_0$  is for an initial reading, and a secret version of said initial reading is stored after further processing thereof (column 11, line 65 to column 12, line 34),

wherein reading  $P_0$  is different from  $P_i$  for  $i > 0$ , and the secret version of  $P_0$  is different from the secret version of  $P_i$ , such that no identification is possible by a direct comparison of the encrypted data (column 11, line 65 to column 12, line 34).

### ***Conclusion***

32. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

33. The following patents are cited to further show the state of the art with respect to comparing encrypted biometric data, such as:

United States Patent No. 6,076,167 to Borza, which is cited to show a method for improving security in network applications.

United States Patent No. 6,697,947 to Matyas, Jr. et al., which is cited to show multi-party biometric authentication.

United States Patent No. 6,507,912 to Matyas, Jr. et al., which is cited to show multi-party biometric authentication.

34. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (703) 305-7704. The examiner can normally be reached on Monday thru Thursday 7-5.

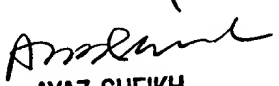
Art Unit: 2131

35. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

36. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christian LaForgia  
Patent Examiner  
Art Unit 2131

clf

  
AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100